UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PROSKAUER ROSE LLP, *Plaintiff*, v. JONATHAN O'BRIEN *Defendant*.	Civil Action No. 1:22-cv-10918

MEMORANDUM OF LAW IN SUPPORT OF JONATHAN O'BRIEN'S
EMERGENCY MOTION FOR PROTECTIVE ORDER

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Defendant Jonathan O'Brien hereby submits this Emergency Motion for Protective Order (the "Motion") to protect the legitimate and reasonable expectation of privacy that he has in the purely personal information contained on his Proskauer-issued iPhone.

PRELIMINARY STATEMENT

In light of the Court's initial analysis (albeit without the benefit of the position below) pertaining to the iPhone password, Mr. O'Brien is providing the password to Proskauer simultaneously with the filing of this Motion.[1] Accordingly, Proskauer's premature Motion to Enforce is now moot.[2] By this Motion, Mr. O'Brien seeks through this motion narrow relief to protect private information – including ***highly private medical photographs of his wife***, personal spousal communications, attorney-client communications about this case, financial information, and other private information, including third party information and trade secrets – contained on his iPhone iPhone – a phone he had for only the last two months of his seven years at Proskauer.[3] As explained below, Proskauer has no legitimate interest in such information, while in contrast, Mr. O'Brien has, under the particular facts and applicable law, a reasonable expectation of privacy.

Mr. O'Brien therefore respectfully requests that the Court order Proskauer to review only Proskauer's information contained on the iPhone (such as his Proskauer Outlook email, calendar, etc.), and prohibit Proskauer from reviewing any of Mr. O'Brien's personal accounts and

---

[1] Mr. O'Brien has asked Proskauer to refrain from reviewing non-Proskauer information pending a ruling on this motion so as not to undermine the ability of the Court to fairly consider this issue.

[2] In the unlikely event that the Court were to determine that the Motion to Enforce is not moot, Mr. O'Brien respectfully requests that the Court consider the instant submission (including the accompanying declaration) as Mr. O'Brien's opposition to that motion as well.

[3] Prior to this, with the exception of a few months in 2015, Mr. O'Brien always used a single phone – his *personal* phone – for both personal purposes and work purposes during his entire seven years until just before he left.

information on the iPhone until further order of the Court or until the parties agree on a forensic protocol. (The parties are almost done negotiating a forensic protocol for the review of information on Mr. O'Brien's personal electronic devices, which can easily be applied to the Proskauer iPhone at issue.)

Good cause for the requested relief exists here for two reasons: (1) Under the caselaw of this Court and the Second Circuit, Mr. O'Brien has a reasonable expectation of privacy in his personal email accounts, text messages, photographs, personal applications, and other non-Proskauer information on his iPhone[4]; and (2) Proskauer has misrepresented the underlying facts of the parties' negotiations on this issue to the Court.

STATEMENT OF FACTS

A brief recitation of the parties' interactions on this issue (with the full corroborating contemporaneous evidence, as opposed to the partial email chains provided by Proskauer) is necessary to demonstrate that (1) Mr. O'Brien was not unreasonably withholding the iPhone password – and indeed tried to provide it in a way that would give Proskauer access to its information on the iPhone; (2) that the parties were actively negotiating the forensic protocol up until the filing of Proskauer's Motion to Enforce the Temporary Restraining Order (Dkt. No. 37); and (3) that it was both premature and unnecessary for Proskauer to seek relief from the Court for the iPhone password.

[4] Proskauer's position is broad enough to encompass even Proskauer's access to the applications on Mr. O'Brien's iPhone – not just his personal email application and text messages, but also applications such as Facebook, Instagram, financial and banking applications, medical applications, etc. *See* O'Brien Decl. ¶ 5. Hopefully, Proskauer's intent was not to encompass live access to this sort of personal information, but out of an abundance of caution given Proskauer's overreaching tactics in this case, Mr. O'Brien vehemently rejects any assertion or suggestion that Proskauer is entitled to access any of that information. *See infra* at pp. 7-12.

Before Mr. O'Brien returned from Mauritius on Thursday, January 5, 2023, earlier in the day, undersigned counsel asked opposing counsel for an inventory of the devices that Proskauer had issued to Mr. O'Brien to ensure a complete return of all devices. *See* Exhibit A. Unfortunately, although Proskauer's counsel said during at least one phone call that they would provide such an inventory, they never did. Mr. O'Brien nevertheless made his best efforts to retrieve all hard copies of Proskauer's information that was in his personal possession, as well as all devices and equipment that had been issued to him. Mr. O'Brien returned all such items that he could locate – including his newly-issued Proskauer iPhone 14 – to Proskauer by 5:00 p.m. on Friday, January 6, 2023, as required.[5]

In an email sent by Mr. O'Brien's counsel to Proskauer's counsel that day (January 6), she explained:

> As to the items being picked up from Mr. O'Brien today, one device is a phone. While it was a Proskauer-issued phone (and is, accordingly, being returned today), Mr. O'Brien was permitted to (and did) use it as a personal phone as well. I am sure there is also personal information on some of the other devices. I expect it goes without saying, but we expect that Mr. O'Brien's personal information, including *e.g.* texts and financial documents, will not be touched by your firm or anyone else absent a negotiated protocol. If you disagree, let's discuss early next week. *See* Exhibit B.

On the same day, January 6, 2023, Mr. O'Brien's counsel emailed a draft forensic protocol to Proskauer's counsel. *See* Exhibit C.

[5] It is worth noting that counsel for Proskauer inappropriately asked Mr. O'Brien – directly, without counsel present – for the iPhone password when counsel for Proskauer collected the iPhone and other devices from Mr. O'Brien's home. *See* Exhibit A. As a represented party, it is unquestionable that counsel for Proskauer should have directed their inquiry to Mr. O'Brien's counsel. *See* N.Y. R. of Professional Conduct 4.2(a).

Late in the afternoon of Sunday, January 8, 2023 – after Mr. O'Brien had searched for Proskauer devices and returned them to Proskauer in accordance with the *ex parte* TRO – Proskauer's counsel belatedly sent an inventory of all Proskauer devices that had been issued to Mr. O'Brien and demanded an explanation as to why "a Proskauer power pack (Serial No. 1Z81RF280312077945) and two Proskauer HP monitors (Serial Nos. CNC01635BP, CBC01635BW)" had not been returned. *See* Exhibit D. These particular items – which plainly had no information on them – had been inadvertently overlooked by Mr. O'Brien during his search.[6] Mr. O'Brien quickly found and returned these remaining Proskauer items to them.

In the same Sunday afternoon (January 8, 2023) email, Proskauer's counsel also demanded the password for the Proskauer iPhone that had been returned by Mr. O'Brien. *See* Exhibit D.

In her response the next morning (Monday, January 9), Mr. O'Brien's counsel explained that she did not currently have the password. *See* Exhibit D. She also reiterated that she would provide the password upon confirmation that Proskauer would refrain from reviewing Mr. O'Brien's personal information or information belonging to third parties on the iPhone until a forensic protocol had been agreed upon – not Proskauer's information, which they would have been free to do with immediate, unfettered access. These are the very same privacy concerns that were the basis for a forensic protocol to govern the review, search for, and deletion of any Proskauer information on Mr. O'Brien's personal devices.

Had Proskauer's counsel simply provided this confirmation at the outset, Proskauer could have had the iPhone password the same day. Proskauer's counsel never gave any such assurance

[6] Proskauer's suggestion that Mr. O'Brien's inadvertent retention of two monitors and a battery pack is evidence of nefarious intent to either misappropriate its confidential information or to defy the terms of the TRO makes as little sense as complaining about a failure to return a Proskauer paper clip. This is hardly the smoking gun that Proskauer attempts to depict it as.

that day, however, or in the days that followed. Instead, Proskauer claimed an unfettered right of access to all of Mr. O'Brien's, his wife's, and third-parties' private information.

On the afternoon of January 9, 2023, counsel for the parties had a call to discuss, in part, the issues raised in the January 8th email. Following that call, the parties exchanged emails setting forth their positions. *See* Exhibit D. Mr. O'Brien's counsel reiterated points she had made during their call, specifically: "***Mr. O'Brien does not seek to prevent Proskauer in any way whatsoever from reviewing and accessing Proskauer information.*** We are only asking for confirmation that Proskauer will ***not review Mr. O'Brien's personal information and communications absent a reasonable protocol***." *Id.* (emphasis added).

Her email continued by stating that in the event the parties reached an impasse on the issue, Mr. O'Brien's counsel would send a draft joint letter setting out Mr. O'Brien's position so that Proskauer could insert its own position, and then the parties could jointly submit the letter to the Court, in compliance with this Court's procedural rules. *Id.*

Mr. O'Brien's counsel also asked about the status of the proposed forensic protocol, as Proskauer had not yet provided comments on the draft circulated days earlier.

Proskauer's counsel finally responded to the forensic protocol proposed by Mr. O'Brien's counsel on the late afternoon of Tuesday, January 10, 2023. *See* Exhibit D.

In addition to attaching a heavily marked-up version of the forensic protocol, Proskauer's counsel represented, "***We will get back to you on next steps concerning the iPhone password***." *Id.* (emphasis added). This was the ***last statement*** that Mr. O'Brien's counsel heard from Proskauer's counsel on the password issue before Proskauer filed its Motion to Enforce (Dkt. No. 37) three days later, on the Friday night of a three-day weekend.

Before that, however, having heard no update on the iPhone password issue, Mr. O'Brien's counsel invited a conversation to further discuss the issue on Thursday, January 12, 2023, and she suggested that Proskauer's counsel work on narrowing the search terms in the interim. *See* Exhibit D. Mr. O'Brien's counsel closed the email by asking if Proskauer's counsel had been able to reach an agreement on the password issue, or whether the parties could continue making progress on that issue with another discussion. *Id.* Again, having received no response to her email, Mr. O'Brien's counsel reached out again later in the day to request a call for January 12, 2023, during which the parties could "plan to discuss the protocol and the phone." *See* Exhibit F.

Proskauer's counsel eventually responded to the repeated requests for a conversation, and the parties scheduled a call for January 12, 2023. During that call, Proskauer's counsel rejected the request to narrow their search terms by stating that they "did not want to bid against" themselves. Tishler Decl. ¶ 10. When counsel for Mr. O'Brien asked counsel for Proskauer if they had any other updates to discuss, counsel for Proskauer stated they did not. *Id.* ¶ 12.

Mr. O'Brien's counsel did not hear from Proskauer again until 6:45 p.m. on Friday, January 13, 2023, when Proskauer's counsel emailed to schedule a phone call for an unspecified purpose. *See* Ex. E.

Mr. O'Brien's counsel responded 19 minutes later, at 7:04 p.m., making themselves available for a call in five minutes and providing a conference line number for all counsel to dial into. Proskauer's counsel neither replied to this email, nor did they dial into the conference line at 7:10 p.m.

Instead, just ten minutes after Mr. O'Brien's counsel sent his email, Proskauer's counsel (around 7:15 p.m.) filed the Motion to Enforce, and, over the next hour, continued to file supporting papers.

Proskauer's counsel did not reply to the email for the rest of the evening, waiting until 7:28 a.m. Saturday morning to do so, saying that he had not seen it because he was "at dinner." *Id.*

Just as Mr. O'Brien first learned of this lawsuit through a reporter asking for comment, counsel for Mr. O'Brien first learned of Proskauer's Motion to Enforce through the automatic ECF notification, despite the parties' ongoing and contemporaneous communications.

ARGUMENT

A. Proskauer Has "No Sound Basis In Fact, Law, Or Logic" To Assert It Has Unfettered Access To All Of Mr. O'Brien's Personal Information or Third Party Information On His Proskauer-issued iPhone.

Proskauer's premise that Mr. O'Brien had "no reasonable expectation of privacy, no privacy rights or privilege protection (including the spousal and attorney-client privileges) regarding the content of [the] [*sic*] Proskauer-owned iPhone," Dkt. 37 at 4, is flatly wrong, and as this Court held in a remarkably similar case, has "no sound basis in fact, law, or logic." *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 559-562 (S.D.N.Y. 2008) ("*Pure Power*").

Each of the cases Proskauer cites on page 4 of its Motion to Enforce dealt with the issue of personal information either (1) sent over a company's internal email or (2) stored on a company computer that was exclusively for company use.[7] *See* Dkt. No. 37 at 4 (citing cases). ***None*** of Proskauer's cited authorities deals with the issue of personal content on mixed-use devices, and

[7] One of those cases was *In re Reserve Fund Securities and Derivative Litigation*, 275 F.R.D. 154, 165, n. 6 (S.D.N.Y. 2011), which the Court also cited at the January 26, 2023 hearing for the proposition that "case law in this district states that where company policy advises employees that their communications on company devices or using company software are not confidential, such communications are not subject to privilege." Jan. 24, 2023 Hr'g Tr. at 6:21-7:1; Dkt. No. 37 at 4. Mr. O'Brien agrees that any e-mails sent over his ***Proskauer email account*** would not be protected by a reasonable expectation of privacy, or otherwise-applicable privileges. At issue here, however, are Mr. O'Brien's ***personal email accounts***, text messages, photos, and other purely personal information on his iPhone.

none deal with the issue of personal content on mixed-use devices that is contained in, for example, personal applications that are on the device (such as Instagram, Facebook, Gmail, etc.), which are the issues facing the Court here.

In reality, the caselaw of this District and Circuit is clear that ***employees do have a reasonable expectation of privacy for personal emails and other information on accounts maintained by outside electronic communication service providers (such as Hotmail), even when accessed on a company device***. *See, e.g.*, *Pure Power*, 587 F. Supp. 2d at 559-562 (determining that former employee had a reasonable expectation of privacy over his personal email accounts even though he accessed them from a work computer); *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001) (holding that employee "had a reasonable expectation of privacy in the contents of his office computer" despite a policy banning use of office equipment for personal use); *United States v. Mendlowitz*, No. 17 CR. 248 (VSB), 2019 WL 1017533, at *7 (S.D.N.Y. Mar. 2, 2019) (despite policy notifying employees that contents of and communications over company computers were not private, holding that "Mendlowitz has demonstrated a sufficient privacy interest with regard to the materials seized from his office and computers but not with regard to the computers and materials seized from the offices of other employees or the CPS servers generally."); *see also Curto v. Medical World Comms.*, No. 03 Civ. 6327 (DRH) (MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (employee's emails stored on company computer, which was at employee's home, were covered by attorney-client privilege despite policy notifying employees that they waived "any right of privacy" to anything on the computers).

This Court's decision in *Pure Power* is instructive. In that case, a former employee was accused of trade secret theft and breach of fiduciary duties (among other counts) in connection with his termination and subsequent opening of a competitive business. *Pure Power*, 587 F. Supp.

2d at 552-53. After the defendant was fired, his former supervisor accessed and printed emails from his personal email accounts (including Hotmail and Gmail), which she was able to do because the former employee had saved his username and password information on the company computers. *Id.* The former employer plaintiff considered those emails "critical to their case." *Id.* at 553. The Company had an Employee Handbook with language remarkably similar to Proskauer's:

> ***e-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over the system. This includes the use of personal e-mail accounts on Company equipment.*** The Company, in its discretion as owner of the E–Mail system, reserves the right to review, monitor, access, retrieve, and delete any matter stored in, created on, received from, or sent through the system, for any reason, without the permission of any system user, and without notice.

Id. at 553-54 (emphasis added). The former employee defendant sought the preclusion and return of the emails, claiming violations of state and federal law, and that some of the emails were protected by attorney-client privilege. *Id.* at 554.

The Court agreed with the defendant that the company's unauthorized access of his personal email was a violation of the Stored Communications Act, 18 U.S.C. § 2701, *et seq.* ("SCA"), which is part of the Wiretap Act. *Id.* at 555-57.[8] The Court also rejected both of the plaintiff's arguments that the company was authorized to view and print the defendant's emails because (1) of the company's policy which set forth he had no expectation of privacy in his personal accounts; and (2) even if he had an expectation of privacy, he gave the company implied consent to access his personal accounts by saving his username and password on company

[8] Given the breadth of Proskauer's request for access to all content on the iPhone, the SCA may be implicated and, to the extent it is, should bar Proskauer's efforts to obtain unfettered access to the phone.

computers. *Id.* at 559-62 ("These arguments have no sound basis in fact, law, or logic."). First, the Court held that according to the company's own policy, its access to personal information "could not apply to e-mails on systems maintained by outside entities such as Microsoft or Google," because there was no evidence that the emails were "created on, sent through, or received from" the company's computers. *Id.* at 559. Second, the Court rejected plaintiff's implied consent theory, analogizing it to the defendant leaving a key to his house on the front desk of the company: "one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings. And, to take the analogy a step further, had the person rummaging through the belongings in [defendant's] house found the key to [his] country house, could that be taken as authorization to search his country house. We think not." *Id.* at 561-62.

Here, Mr. O'Brien was using a Proskauer-issued iPhone that was specifically given to him for both professional ***and personal use***. O'Brien Decl. ¶¶ 4, 18-21. Mr. O'Brien used it appropriately in both capacities. *Id.* It bears repeating that Mr. O'Brien is ***not contesting Proskauer's access to his Proskauer email account, his Proskauer-related applications, or any Proskauer files or information stored on any of the above***. *Id.* ¶¶ 9, 14. What Mr. O'Brien is trying to achieve is simply protection over his personal information, and that of third parties. Furthermore, he never waived his privacy rights over such information by responding "Fine with me" to an email asking him to review and approve revisions to Proskauer's Computer and Communications Use and Data Protection Policy ("the Policy") or by later signing an acknowledgment of his receipt of the Policy.[9]

[9] To further illustrate Mr. O'Brien's position and the relief sought through this Motion, Proskauer is in possession of Mr. O'Brien's work laptop. Mr. O'Brien ***does not challenge*** Proskauer's review of that laptop, as it is very different from the iPhone that he was permitted to

As the *Pure Power* court instructed, Proskauer's aggressive position is unsupportable in fact, logic, and law. By its own terms, the section of the Policy that Proskauer selectively quotes in the Motion states that the expectation of privacy is waived only "[t]o the extent permitted by law" for "data, content and materials on it or transmitted through it." (Dkt. No. 38-1 at § 9.10.2.) Proskauer's current request is not limited to Mr. O'Brien's information "on" or "transmitted through" the iPhone. It seeks access to ***everything*** on the iPhone. *See* Dkt. No. 37 at 4 (asserting Proskauer has access to all "content" on the iPhone). As in *Pure Power*, Proskauer has shown no evidence (nor has it even alleged) that any of Mr. O'Brien's personal information was transmitted through the iPhone, or that any of it is actually contained on it. Even under Proskauer's own Policy, Proskauer's request is far too broad to be permissible. *See Pure Power*, 587 F. Supp. 2d at 559.

For similar reasons, Proskauer's position that Mr. O'Brien has waived his spousal and attorney-client privileges as to personal email or text communications that may exist on his Proskauer iPhone should be rejected.[10] The cases cited by Proskauer on this point involve an employee's use of his or her ***work email account*** to communicate with spouses or attorneys, which is not the issue here. Further, third parties with whom Mr. O'Brien has communicated via his

use, and did use, for personal purposes. This distinction is especially salient given the nature of the information stored on the iPhone, as described above and in Mr. O'Brien's Declaration.

[10] Moreover, New York courts have found that an employee's use of an employer's computer for personal purposes does not, standing alone, constitute a waiver of attorney work product protections where no *actual* disclosure had been made and where, although an employer reserved a right of access to information on a company laptop computer, the employer did not exercise that right as to the laptop and never actually viewed any of the documents stored on that laptop. *See Miller v. Zara USA, Inc.*, 151 A.D.3d 462, 463 (1st Dep't. 2017); *Peerenboom v. Marvel Entertainment, LLC*, 148 A.D.3d 531, 532 (1st Dep't. 2017). Thus, Proskauer would, at a minimum, need to demonstrate that it had actually previously exercised its right to access and view documents stored on Mr. O'Brien's Proksauer-issued iPhone in order to prove a waiver of communications containing attorney work product. Proskauer has not done this.

personal email accounts or text messages (using his personal cellphone number – not one issued by the firm, *see* O'Brien Decl. ¶ 21) have an interest in protecting the privacy of their own confidential information that may reside in those personal accounts. For example, certain information shared by Paul Hastings with Mr. O'Brien through his personal email account is subject to a nondisclosure agreement. O'Brien Decl. ¶ 16. Paul Hastings has an independent interest in preventing its own proprietary, confidential and/or trade secret information from being disclosed to a competitor like Proskauer, and Proskauer has not pointed to any authority to suggest that this Court should not uphold the confidentiality of such third-party information in this context.[11]

B. Mr. O'Brien Did Not Violate The TRO By Withholding The iPhone Password.

Mr. O'Brien has already fully complied with the terms of the *ex parte* TRO. (Dkt. No. 15.)

In Paragraph 2 of the TRO, the Court ordered that Mr. O'Brien:

> ***is temporarily restrained from continuing to possess and shall return to Proskauer***, by no later than January 5, 2023 at 12:00 noon, ***any and all of Proskauer's proprietary, confidential and/or trade secret information (including copies thereof) that Mr. O'Brien*** and/or subordinates at his direction copied, printed or otherwise ***obtained from Proskauer's computer systems***, including all copies of Proskauer's electronic files and all paper copies in his possession (including the two USB drives to which Mr. O'Brien and/or subordinates at his direction copied Proskauer information on December 5, 2022 and December 16, 2022, and any electronic or paper copies of files on those drives). *Id.* (emphasis added).

By the TRO's terms, what Proskauer sought (and what the TRO – written by Proskauer – granted) is the return of any and all of Proskauer's purportedly proprietary, confidential and/or trade secret information that Mr. O'Brien had obtained from the firm's computer systems – and

[11] When discovery proceeds (the process to which Proskauer's cases relate), there are ways to ensure that Proskauer receives only that information that may be discoverable, as opposed to the wholesale, unfettered access to everything that Proskauer is now trying to obtain.

two USB drives, in particular – so that Mr. O'Brien no longer had it in his possession (or presumably had access to it).[12] Accordingly, Mr. O'Brien fully complied with the language of the TRO when he returned all paper copies and electronic devices containing Proskauer's information – ***including his Proskauer iPhone*** – to the firm on January 6, 2023.[13]

To the extent that the TRO's language was susceptible of a broader interpretation to include the return of the password, the language was not clear in that regard, and given that it was drafted by Proskauer and is an order, should be read narrowly.[14] Moreover, it was only Proskauer's conduct in refusing to refrain from looking at non-Proskauer information that prevented Mr. O'Brien from providing the password. This entire dispute could have been avoided had Proskauer simply said, "Okay." Alternatively, the issue could have been raised with Court in accordance with its Individual Rules pertaining to such disputes – *as Mr. O'Brien asked Proskauer to do* before Proskauer jumped the gun and filed their motion (without telling the Court where the discussions actually stood).

---

[12] It cannot be – certainly at the *ex parte* TRO stage – that the Court was ordering not only removal of the information from Mr. O'Brien's possession, but full access for Proskauer to Mr. O'Brien's personal information, privileged communications, and third party private and trade secret information.

[13] As discussed previously, the fact that two Proskauer computer monitors and a powerpack were returned a few days after January 6, 2023 is not evidence of Mr. O'Brien's noncompliance with the TRO, as there is no Proskauer proprietary, confidential and/or trade secret information residing on such pieces of equipment. Of course, had Proskauer actually cared about getting back any such equipment (as opposed to what an *ex parte* TRO is actually designed to do), Proskauer could have simply provided the requested inventory identifying each device and piece of equipment issued to Mr. O'Brien. Unfortunately, Proskauer did not do so until *after* the January 6th deadline had passed. *See* Ex. D. Even then, Mr. O'Brien promptly located the two monitors and battery pack and returned them.

[14] While Mr. O'Brien maintains this concern, given the Court's initial analysis (which, with respect, was made without the benefit of the factual context, law, and arguments set forth in this Memorandum), Mr. O'Brien has provided the password, and seeks protection through this emergency Motion.

Paragraph 4 of the TRO, which addresses Mr. O'Brien's *personal* email accounts and other personal electronic devices, requires him to "permit the permanent removal, deletion, and destruction of all copies of Proskauer's electronic files or information transmitted to Mr. O'Brien's computers or personal email accounts or otherwise in his possession, subject to the supervision of Proskauer, so as to preserve evidence of all such files or information." *Id.* As reported to the Court in connection with the continuance of the hearing, the parties agreed to attempt to negotiate a forensic protocol to accomplish this process, which is nearly complete. *See* Dkt. No. 22 at 1.

Parties routinely negotiate mutually-agreeable forensic protocols under these circumstances in acknowledgment of the obvious privacy rights that individuals have in the personal information in their personal accounts and on their personal devices. As indicated above, Mr. O'Brien's counsel has diligently and in good faith engaged in discussions with Proskauer's counsel to reach such a protocol since January 6, 2023 to ensure that any of Proskauer's information that may reside in Mr. O'Brien's personal email account or elsewhere on his personal devices can be promptly searched for, removed, deleted, and/or destroyed in compliance with the TRO without violating his privacy rights. *See* Ex. C.

Because identical privacy interests are involved – regardless of whether Mr. O'Brien's personal email account, for example, resides in an application on his Proskauer iPhone or a personal phone – and anticipating that Proskauer might take the unreasonable, untenable position it is currently taking, Mr. O'Brien's counsel requested confirmation from Proskauer that it would refrain from reviewing Mr. O'Brien's personal email account and other personal or third-party information on his Proskauer iPhone until a forensic protocol was in place.[15] *Id.*

[15] It is fairly common for employees to use Proskauer-issued devices for both personal and work purposes, and it is apparently common for employees leaving Proskauer to return completely wiped Proskauer-issued phones in the interest of protecting their personal information. O'Brien

Rather than provide this confirmation or focus their energies on arriving at a mutually-agreeable forensic protocol, Proskauer's counsel instead decided to stretch out negotiations regarding the protocol for over a week, lead Mr. O'Brien's counsel to believe that the password was still an open issue, and surreptitiously prepare the instant Motion.

Relatedly, Mr. O'Brien was attempting to comply with the terms of the TRO when he removed Proskauer's mobile device management agent (an application that the firm installs on Proskauer-issued devices) from his Proskauer-issued iPhone on December 30, 2022.[16] O'Brien Decl. ¶¶ 9-13. Once he learned about this lawsuit and the *ex parte* TRO, Mr. O'Brien was understandably concerned that he would be violating a Court order if he were to even inadvertently access Proskauer's computer systems through any of the Proskauer applications on his iPhone. *Id.* ¶ 9. Consequently, Mr. O'Brien, who is not a lawyer (and believing he was acting consistent with the Court's Order) removed the Proskauer agent to ensure that, consistent with the TRO, he would not have possession of Proskauer's information, or be able to access Proskauer's systems, via his iPhone. *Id.* ¶¶ 2, 9, 13. It was particularly important to him that his iPhone not continue to be linked to Proskauer's systems because it was the only phone that he had with him in Mauritius, and he needed to be able to continue using it for personal reasons (including to coordinate his

---

Decl. ¶ 22. Mr. O'Brien did not wipe his phone; he returned it intact with all of his and third parties' confidential, private, and personal information on it. *Id.*

[16] Remarkably, despite Proskauer's allegations of criminal-level misappropriation by Mr. O'Brien, *see* Dkt. No. 6, and the issuance of the *ex parte* TRO on December 28, 2022, it appears from the Declarations filed with Dkt. No. 37 that *Proskauer neglected to make any attempt to remove Mr. O'Brien's access to its computer system until December 30, 2022*. O'Brien Decl. ¶ 10. The fact that Proskauer permitted Mr. O'Brien to have continued access to its systems ***for days after*** the issuance of the *ex parte* TRO seriously undermines its contention that Mr. O'Brien posed any threat to its purportedly confidential information and/or trade secrets, let alone a threat of irreparable harm. By deleting the app from his Proskauer-issued iPhone and thereby removing his access to Proskauer's systems, Mr. O'Brien took greater pains to protect Proskauer's information that it did for itself. O'Brien Decl. ¶¶ 9-10.

defense in this litigation) while he remained out of the country. *Id.* ¶ 12. To be clear, Mr. O'Brien knew that deleting the mobile device management agent from the Proskauer iPhone did not result in the deletion of any Proskauer information—all of that information still resides, and remains accessible to Proskauer, on its systems. *Id.* ¶ 9.

In short, Proskauer has everything that it originally requested from the Court. If Proskauer wanted Mr. O'Brien to provide passwords to his Proskauer-issued devices without any conditions, and with explicit access to comb through all of Mr. O'Brien's personal email account and other personal information without restrictions (something it could not even achieve through discovery), it ***could and should have*** expressly sought such relief as part of its original *ex parte* TRO motion. It failed to do so, and the Court accepted Proskauer's terms. Mr. O'Brien's valid and reasonable understanding of the language of the order and his privacy expectations should not be set aside now that Proskauer has decided to rewrite and expand what it asked for.

Finally, there is no time-sensitivity to Proskauer's access to Mr. O'Brien's personal information, and Proskauer's exaggerated statement that the iPhone has "functionally and effectively not been returned to Proskauer" (Dkt. No. 37 at p. 2), rings hollow. The TRO is aimed at moving Proskauer's proprietary, confidential, and/or trade secret information out of Mr. O'Brien's hands to prevent its further use and dissemination. Proskauer now has the Proskauer-issued iPhone at issue, so there is no further risk of its contents being accessed, used, or disclosed by Mr. O'Brien. And, for that purpose, *i.e.*, the purpose of the TRO, what may or may not be on that iPhone is largely irrelevant at this stage in the proceedings.

CONCLUSION

For all of the reasons set forth above, Mr. O'Brien respectfully requests the Court issue an emergency order of protection prohibiting Proskauer from accessing Mr. O'Brien's personal

accounts, applications, and information on the Proskauer-issued iPhone, until the parties have agreed on a forensic protocol for the review of that information.

Dated: January 26, 2023

Respectfully submitted,

BECK REED RIDEN LLP

/s/ *Russell Beck*

Russell Beck
Sarah C. C. Tishler
BECK REED RIDEN LLP
155 Federal Street, Suite 1302
Boston, Massachusetts 02110
Telephone: (617) 500-8660
Facsimile: (617) 500-8665
rbeck@beckreed.com
tishler@beckreed.com

Russell M. Yankwitt
Michael H. Reed
YANKWITT LLP
140 Grand Street, Suite 705
White Plains, New York 10601
Tel: (914) 686-1500
Fax: (914) 487-5000
russell@yankwitt.com
michael@yankwitt.com

Attorneys for Jonathan O'Brien